

# Symmetrizing Cost of Quantum States

Eyuri Wakakuwa\*

Department of Communication Engineering and Informatics,  
Graduate School of Informatics and Engineering,  
The University of Electro-Communications, Japan  
(Dated: November 2, 2016)

We introduce and analyze a task that we call *symmetrization*, in which a state of a quantum system, associated with a symmetry group, is transformed by a random unitary operation to a symmetric state. Each element of the unitary ensemble is required to be symmetry-preserving, in the sense that it maps any symmetric state to another. We consider an asymptotic limit of infinitely many copies and vanishingly small error, and analyze the *symmetrizing cost*, that is, the minimum cost of randomness per copy required for symmetrization. We derive a single-letter formula for the symmetrizing cost of an arbitrary quantum state, by proving that it is equal to the relative entropy of frameness.

PACS numbers: 03.65.Ta, 03.67.-a

## I. INTRODUCTION

The concept of symmetry has played significant roles in the development of modern physics, encompassing particle physics, condensed matter theory and cosmology. A quantum state is called *symmetric* if it is invariant under the action of a given symmetry group; otherwise it is called *asymmetric*. Asymmetric quantum states can be exploited as resources for quantum information processing tasks, such as quantum metrology[1, 2] and communication requiring the shared reference frame[3–8].

In this paper, we address a question of how to quantify asymmetry of quantum states operationally, following the lines of [8–13]. To this end, we introduce a task that we call *symmetrization*, in which a quantum state is transformed by a random unitary operation to a symmetric state (FIG.1). Each element of the unitary ensemble is required to be symmetry-preserving, i.e., it maps any symmetric state to another. We consider an asymptotic scenario of infinitely many copies and vanishingly small error, and analyze the *symmetrizing cost*, that is, the minimum cost of randomness per copy required for symmetrization. We prove that the symmetrizing cost of a state is equal to the *relative entropy of frameness*, which is a measure of asymmetry introduced in [10]. Our approach is a generalization of that of [14], in which the coherence of quantum states was analyzed in a similar operational framework.

This paper is organized as follows. In Section II, we review mathematical treatments of symmetry and asymmetry of quantum states. In Section III, we introduce the formal definitions of symmetrization and the symmetrizing cost, and describe the main result. A proof of the main result is provided in Section IV and VI separately, with a mathematical preparation in Section V. Conclusions are given in Section VII.

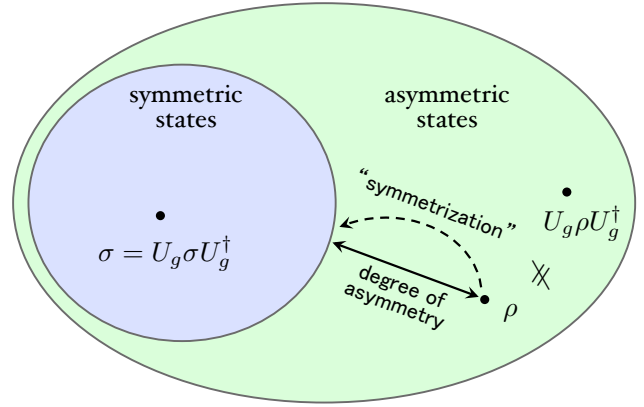


FIG. 1: A schematic diagram of the problem addressed in this paper is depicted. For a given symmetry group  $G$  with a unitary representation  $\{U_g\}_{g \in G}$ , states of a quantum system are classified into two categories: one that is invariant under the action of  $U_g$  for all  $g \in G$  (symmetric states), and the other that is not (asymmetric states). *Symmetrization* is a task in which an asymmetric state  $\rho$  is transformed to a symmetric state by a random application of unitary operations that keep the set of symmetric states invariant (Definition 1 in Section III). We quantify the degree of asymmetry of the state  $\rho$  by the minimum cost of randomness required for symmetrizing it, in an asymptotic limit of infinitely many copies and vanishingly small error. We prove that the cost function is equal to the relative entropy of frameness  $D_{\text{fr}}(\rho) := \min_{\sigma} D(\rho||\sigma)$ , where the minimization is taken over all symmetric states  $\sigma$  (Theorem 2 in Section III).

Throughout this paper, we consider a quantum system  $A$  described by a Hilbert space  $\mathcal{H}^A$  with dimension  $d (< \infty)$ , and a symmetry group  $G$  with associated unitary representation  $\{U_g\}_{g \in G}$  on  $\mathcal{H}^A$ .

*Notations.*  $\mathcal{S}(\mathcal{H})$  denotes the set of normalized state on a Hilbert space  $\mathcal{H}$ , and  $\mathcal{U}(\mathcal{H})$  denotes the set of unitary operators on  $\mathcal{H}$ . A system composed of  $n$  identical systems of  $A$  is denoted by  $A^n$ . The Shannon entropy of

\*Electronic address: wakakuwa@quest.is.uec.ac.jp

a probability distribution  $\{p_j\}_j$  is denoted as  $H(\{p_j\}_j)$ , and the von Neumann entropy of a state  $\rho^A$  is interchangeably denoted by  $S(\rho^A)$  and  $S(A)_\rho$ .  $\log x$  represents the base 2 logarithm of  $x$ .

## II. SYMMETRY OF QUANTUM STATES

In this section, we review mathematical definitions of symmetry and asymmetry of quantum states.

### A. Unipartite System

A state  $\sigma \in \mathcal{S}(\mathcal{H}^A)$  is said to be *symmetric* if it satisfies

$$U_g \sigma U_g^\dagger = \sigma, \forall g \in G,$$

and said to be *asymmetric* otherwise. We denote the set of symmetric states by  $\mathcal{S}_{\text{inv}}(G)$ , i.e.,

$$\mathcal{S}_{\text{inv}}(G) := \{\sigma \mid \forall g \in G : U_g \sigma U_g^\dagger = \sigma, \sigma \in \mathcal{S}(\mathcal{H}^A)\}.$$

We define a unitary  $V$  acting on  $\mathcal{H}^A$  to be *symmetry-preserving* if it satisfies

$$V \sigma V^\dagger \in \mathcal{S}_{\text{inv}}(G), \forall \sigma \in \mathcal{S}_{\text{inv}}(G).$$

We denote the set of symmetry-preserving unitaries by  $\mathcal{U}_{\text{SP}}(G)$ , i.e.,

$$\begin{aligned} \mathcal{U}_{\text{SP}}(G) &:= \\ \{V \mid \forall \sigma \in \mathcal{S}_{\text{inv}}(G) : V \sigma V^\dagger \in \mathcal{S}_{\text{inv}}(G), V \in \mathcal{U}(\mathcal{H}^A)\}. \end{aligned}$$

Let  $\mathcal{T}$  be a quantum operation on  $\mathcal{S}(\mathcal{H}^A)$  defined by

$$\mathcal{T}(\tau) = \int_G dg U_g \tau U_g^\dagger, \forall \tau \in \mathcal{S}(\mathcal{H}^A), \quad (1)$$

with  $dg$  being the group invariant (Haar) measure.  $\mathcal{T}$  is called the *twirling operation*. It follows that

$$\mathcal{T}(\rho) \in \mathcal{S}_{\text{inv}}(G), \forall \rho \in \mathcal{S}(\mathcal{H}^A). \quad (2)$$

By definition, we also have

$$\mathcal{T}(\sigma) = \sigma, \forall \sigma \in \mathcal{S}_{\text{inv}}(G). \quad (3)$$

### B. $n$ Identical Systems

We say that a state  $\sigma \in \mathcal{S}((\mathcal{H}^A)^{\otimes n})$  is *symmetric* if it satisfies

$$U_{\vec{g}} \sigma U_{\vec{g}}^\dagger = \sigma, \forall \vec{g} \in G^n, \quad (4)$$

where we introduced notations  $\vec{g} := (g_1, \dots, g_n)$  and

$$U_{\vec{g}} := U_{g_1} \otimes \dots \otimes U_{g_n} \quad (5)$$

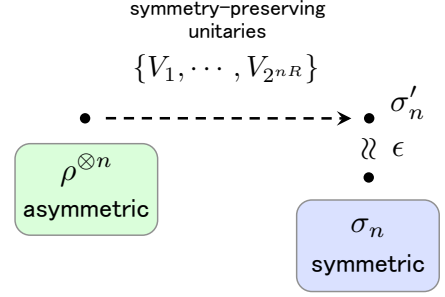


FIG. 2: A schematic diagram of the task of symmetrization is depicted.  $n$  copies of an asymmetric state  $\rho$  is transformed by a random application of symmetry-preserving unitaries  $\{V_1, \dots, V_{2^{nR}}\}$  with the uniform distribution. We require that the state after the transformation is a symmetric state  $\sigma_n$  up to a small error  $\epsilon$ . The symmetrizing cost of  $\rho$  is defined as the minimum rate  $R$  such that  $\epsilon \rightarrow 0$  can be accomplished in the limit of  $n \rightarrow \infty$ , by properly choosing  $\{V_1, \dots, V_{2^{nR}}\}$  and  $\sigma_n$  for each  $n$ .

for  $g_i \in G$  ( $i = 1, \dots, n$ ). We denote the set of symmetric states on  $A^n$  by  $\mathcal{S}_{\text{inv}}(G, n)$ , i.e.,

$$\begin{aligned} \mathcal{S}_{\text{inv}}(G, n) &:= \\ \{\sigma \mid \forall \vec{g} \in G^n : U_{\vec{g}} \sigma U_{\vec{g}}^\dagger = \sigma, \sigma \in \mathcal{S}((\mathcal{H}^A)^{\otimes n})\}. \end{aligned}$$

We define a unitary  $V$  acting on  $(\mathcal{H}^A)^{\otimes n}$  to be *symmetry-preserving* if it satisfies

$$V \sigma V^\dagger \in \mathcal{S}_{\text{inv}}(G, n), \forall \sigma \in \mathcal{S}_{\text{inv}}(G, n).$$

We denote the set of symmetry-preserving unitaries on  $(\mathcal{H}^A)^{\otimes n}$  by  $\mathcal{U}_{\text{SP}}(G, n)$ , that is,

$$\begin{aligned} \mathcal{U}_{\text{SP}}(G, n) &:= \{V \mid \forall \sigma \in \mathcal{S}_{\text{inv}}(G, n) : V \sigma V^\dagger \in \mathcal{S}_{\text{inv}}(G, n), \\ &\quad V \in \mathcal{U}((\mathcal{H}^A)^{\otimes n})\}. \end{aligned}$$

By definition, it immediately follows that

$$U_{\vec{g}} \in \mathcal{U}_{\text{SP}}(G, n), \forall \vec{g} \in G^n \quad (6)$$

and

$$\mathcal{T}^{\otimes n}(\tau) = \int_G d\vec{g} U_{\vec{g}} \tau U_{\vec{g}}^\dagger, \forall \tau \in \mathcal{S}((\mathcal{H}^A)^{\otimes n}), \quad (7)$$

where we denoted  $dg_1 \dots dg_n$  by  $d\vec{g}$ , and  $dg_i$  is the  $G$ -invariant (Haar) measure for each  $i$ . In the same way as (2) and (3), we have

$$\mathcal{T}^{\otimes n}(\rho) \in \mathcal{S}_{\text{inv}}(G, n), \forall \rho \in \mathcal{S}((\mathcal{H}^A)^{\otimes n})$$

and

$$\mathcal{T}^{\otimes n}(\sigma) = \sigma, \forall \sigma \in \mathcal{S}_{\text{inv}}(G, n). \quad (8)$$

### III. SYMMETRIZING COST

In this section, we introduce the formal definitions of symmetrization and the symmetrizing cost, and state the main result.

Consider an asymmetric state  $\rho$  on system  $A$ . Symmetrization is a task in which  $n$  copies of  $\rho$  is transformed to a symmetric state by a random application of symmetry-preserving unitary operations (FIG.2). We do not require that the state after the operation is *exactly* a symmetric state for finite  $n$ . Instead, we require that the state is equal to a symmetric state *within a small error* for large  $n$ , and that the error vanishes in the limit of  $n \rightarrow \infty$ . The *symmetrizing cost* is defined as the minimum cost of randomness per copy required for symmetrization. A rigorous definition is given as follows.

*Definition 1* A rate  $R$  is said to be achievable in symmetrizing a state  $\rho \in \mathcal{S}(\mathcal{H}^A)$  if, for any  $\epsilon > 0$  and sufficiently large  $n$ , there exist a symmetric state  $\sigma_n \in \mathcal{S}((\mathcal{H}^A)^{\otimes n})$  and a set of unitary operations  $\{V_k\}_{k=1}^{2^{nR}}$  on  $A^n$  such that  $V_k \in \mathcal{U}_{\text{SP}}(G, n)$  for all  $k \in \{1, \dots, 2^{nR}\}$  and

$$\|\mathcal{V}_n(\rho^{\otimes n}) - \sigma_n\|_1 \leq \epsilon$$

for

$$\mathcal{V}_n : \tau \rightarrow \frac{1}{2^{nR}} \sum_{k=1}^{2^{nR}} V_k \tau V_k^\dagger.$$

The symmetrizing cost of a state  $\rho \in \mathcal{S}(\mathcal{H}^A)$  is defined as

$$C_{\text{sym}}(\rho) := \inf\{R \mid R \text{ is achievable in symmetrizing } \rho\}.$$

The main result of this paper is as follows:

*Theorem 2* For an arbitrary  $\rho \in \mathcal{S}(\mathcal{H}^A)$ , it holds that

$$C_{\text{sym}}(\rho) = D_{\text{fr}}(\rho),$$

where  $D_{\text{fr}}(\rho)$  is the *relative entropy of frameness*[10] defined by

$$D_{\text{fr}}(\rho) := \min_{\sigma \in \mathcal{S}_{\text{inv}}(G)} D(\rho \parallel \sigma). \quad (9)$$

A proof of the converse part of Theorem 2 will be provided in Section IV, and that of the direct part will be given in Section VI after a preparation in Section V. The proofs are based on the following equality that was proved in [10] (see Proposition 2 therein):

$$D_{\text{fr}}(\rho) = D(\rho \parallel \mathcal{T}(\rho)) = S(\mathcal{T}(\rho)) - S(\rho), \quad \forall \rho \in \mathcal{S}(\mathcal{H}^A). \quad (10)$$

As for operational meanings of the relative entropy of frameness, see Section III of [10] and [11].

### IV. PROOF OF OPTIMALITY

The converse part of Theorem 2 is formulated as

$$C_{\text{sym}}(\rho) \geq D_{\text{fr}}(\rho). \quad (11)$$

We prove this inequality by using the following lemma.

*Lemma 3* For any  $\rho \in \mathcal{S}(\mathcal{H}^A)$  and  $V \in \mathcal{U}_{\text{SP}}(G)$ , we have

$$S(\mathcal{T}(V\rho V^\dagger)) = S(\mathcal{T}(\rho)). \quad (12)$$

*Proof:* From Equalities (9) and (10), we have

$$\begin{aligned} S(\mathcal{T}(\rho)) - S(\rho) &= \min_{\sigma \in \mathcal{S}_{\text{inv}}(G)} D(\rho \parallel \sigma), \\ S(\mathcal{T}(V\rho V^\dagger)) - S(V\rho V^\dagger) &= \min_{\sigma' \in \mathcal{S}_{\text{inv}}(G)} D(V\rho V^\dagger \parallel \sigma'). \end{aligned}$$

The unitary invariance of the von Neumann entropy implies

$$S(\rho) = S(V\rho V^\dagger).$$

We also have

$$\begin{aligned} \min_{\sigma' \in \mathcal{S}_{\text{inv}}(G)} D(V\rho V^\dagger \parallel \sigma') &= \min_{\sigma' \in \mathcal{S}_{\text{inv}}(G)} D(\rho \parallel V^\dagger \sigma' V) \\ &= \min_{\sigma \in \mathcal{S}_{\text{inv}}(G)} D(\rho \parallel \sigma). \end{aligned}$$

Hence we obtain (12). ■

It is straightforward to generalize Lemma 3 to obtain that

$$S(\mathcal{T}^{\otimes n}(V\rho V^\dagger)) = S(\mathcal{T}^{\otimes n}(\rho)) \quad (13)$$

for any  $\rho \in \mathcal{S}((\mathcal{H}^A)^{\otimes n})$  and  $V \in \mathcal{U}_{\text{SP}}(G, n)$ .

Inequality (11) is proved as follows. By definition, for any  $R > C_{\text{sym}}(\rho)$ ,  $\epsilon > 0$  and sufficiently large  $n$ , there exist a symmetric state  $\sigma_n \in \mathcal{S}_{\text{inv}}(G, n)$  and a set of unitaries  $\{V_k\}_{k=1}^{2^{nR}}$  such that

$$\|\mathcal{V}_n(\rho^{\otimes n}) - \sigma_n\|_1 \leq \epsilon \quad (14)$$

for

$$\mathcal{V}_n : \tau \rightarrow \frac{1}{2^{nR}} \sum_{k=1}^{2^{nR}} V_k \tau V_k^\dagger,$$

and  $V_k \in \mathcal{U}_{\text{SP}}(G, n)$  for all  $k \in \{1, \dots, 2^{nR}\}$ . Due to the monotonicity of the trace distance and the triangle inequality, it follows from (8) and (14) that

$$\begin{aligned} &\|(\mathcal{T}^{\otimes n} \circ \mathcal{V}_n)(\rho^{\otimes n}) - \mathcal{V}_n(\rho^{\otimes n})\|_1 \\ &\leq \|(\mathcal{T}^{\otimes n} \circ \mathcal{V}_n)(\rho^{\otimes n}) - \sigma_n\|_1 + \|\mathcal{V}_n(\rho^{\otimes n}) - \sigma_n\|_1 \\ &= \|(\mathcal{T}^{\otimes n} \circ \mathcal{V}_n)(\rho^{\otimes n}) - \mathcal{T}^{\otimes n}(\sigma_n)\|_1 + \|\mathcal{V}_n(\rho^{\otimes n}) - \sigma_n\|_1 \\ &\leq 2 \|\mathcal{V}_n(\rho^{\otimes n}) - \sigma_n\|_1 \\ &\leq 2\epsilon. \end{aligned} \quad (15)$$

Let  $E$  be an ancillary system described by a Hilbert space  $\mathcal{H}^E$  with dimension  $2^{nR}$ , and define an isometry  $V : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^E \otimes (\mathcal{H}^A)^{\otimes n}$  by

$$\tilde{V} = \frac{1}{2^{nR}} \sum_{k=1}^{2^{nR}} |k\rangle^E \otimes V_k^{A^n}.$$

Let  $Z$  be a quantum system with dimension  $d = \dim \mathcal{H}^A$ , and let  $|\psi\rangle^{AZ}$  be a purification of  $\rho$ , i.e.,  $\rho = \text{Tr}_Z[|\psi\rangle\langle\psi|^{AZ}]$ . Consider a pure state

$$|\tilde{\psi}_n\rangle^{EA^n Z^n} := \tilde{V} |\psi\rangle^{\otimes n} \otimes |Z^n\rangle.$$

The von Neumann entropies for this state are calculated as follows. First, we have

$$nR = \dim \mathcal{H}^E \geq S(E)_{\tilde{\psi}_n} \geq S(EZ^n)_{\tilde{\psi}_n} - S(Z^n)_{\tilde{\psi}_n}, \quad (16)$$

where the second inequality follows from the subadditivity of the von Neumann entropy. Second, we have

$$S(Z^n)_{\tilde{\psi}_n} = S(Z^n)_{\psi^{\otimes n}} = S(\rho^{\otimes n}) = nS(\rho), \quad (17)$$

since  $\tilde{\psi}_n^{Z^n} = (\psi^Z)^{\otimes n}$  and  $|\psi\rangle^{AZ}$  is a purification of  $\rho$ . Third, we have

$$S(EZ^n)_{\tilde{\psi}_n} = S(A^n)_{\tilde{\psi}_n} = S(\mathcal{V}_n(\rho^{\otimes n})), \quad (18)$$

because  $|\tilde{\psi}_n\rangle$  is a pure state on  $EA^n Z^n$  and

$$\tilde{\psi}_n^{A^n} = \text{Tr}_{EZ^n}[\tilde{\psi}_n] = \mathcal{V}_n(\rho^{\otimes n}).$$

Forth, from Inequality (15) and the Fannes inequality[15], we have

$$S(\mathcal{V}_n(\rho^{\otimes n})) \geq S((\mathcal{T}^{\otimes n} \circ \mathcal{V}_n)(\rho^{\otimes n})) - n\eta(2\epsilon) \log d, \quad (19)$$

where

$$\eta(x) := \begin{cases} x - x \log x & (x \leq 1/e) \\ x + \frac{1}{e} & (x \geq 1/e) \end{cases}.$$

Finally, due to the concavity of the von Neumann entropy and Equality (13), we have

$$\begin{aligned} S((\mathcal{T}^{\otimes n} \circ \mathcal{V}_n)(\rho^{\otimes n})) &\geq \frac{1}{2^{nR}} \sum_{k=1}^{2^{nR}} S(\mathcal{T}^{\otimes n}(V_k \rho^{\otimes n} V_k^\dagger)) \\ &= S(\mathcal{T}^{\otimes n}(\rho^{\otimes n})) = nS(\mathcal{T}(\rho)). \end{aligned} \quad (20)$$

Combining (16), (17), (18), (19) and (20), we obtain

$$nR \geq nS(\mathcal{T}(\rho)) - nS(\rho) - n\eta(2\epsilon) \log d,$$

which implies

$$R \geq D_{\text{fr}}(\rho) - \eta(2\epsilon) \log d$$

due to (10). Since this relation holds for any  $R > C_{\text{sym}}(\rho)$  and small  $\epsilon$ , we obtain Inequality (11).  $\blacksquare$

## V. DECOMPOSITION OF THE HILBERT SPACE

In this section, we present a decomposition of a Hilbert space based on the unitary representation of a symmetry group. The results presented here will be used in Section VI to prove the direct part of Theorem 2.

### A. Direct-Sum Form

The Hilbert space  $\mathcal{H}^A$  is decomposed in the form of the direct sum (see Section II-C of [4]) as

$$\mathcal{H}^A = \bigoplus_{q \in Q} \mathcal{M}_q \otimes \mathcal{N}_q,$$

where  $\mathcal{M}_q$  ( $q \in Q$ ) are Hilbert spaces carrying irreducible representations of  $G$ , and  $\mathcal{N}_q$  ( $q \in Q$ ) are the ones carrying the trivial representations of  $G$ . Correspondingly,  $U_g$  is decomposed as

$$U_g = \bigoplus_{q \in Q} u_{g,q} \otimes I_q, \quad (21)$$

where  $\{u_{g,q}\}_{g \in G}$  is an irreducible representation of  $G$  for each  $q$  and  $I_q$  is the identity operator on  $\mathcal{N}_q$ .

Let  $\pi_q$  be the maximally mixed state on  $\mathcal{M}_q$  for each  $q \in Q$ . Due to Schur's lemma, a state  $\sigma \in \mathcal{S}(\mathcal{H}^A)$  is symmetric if and only if  $\sigma$  is decomposed as

$$\sigma = \bigoplus_{q \in Q} p_q \pi_q \otimes \sigma_q \quad (22)$$

with some probability distribution  $\{p_q\}_{q \in Q}$  and states  $\sigma_q$  on  $\mathcal{N}_q$  for  $q \in Q$ .

### B. Tensor-Product Form

Let us introduce three Hilbert spaces  $\mathcal{H}^{a_0}$ ,  $\mathcal{H}^{a_L}$  and  $\mathcal{H}^{a_R}$  such that

$$\begin{aligned} \dim \mathcal{H}^{a_0} &= |Q|, \\ \dim \mathcal{H}^{a_L} &= \max_q \dim \mathcal{M}_q, \\ \dim \mathcal{H}^{a_R} &= \max_q \dim \mathcal{N}_q. \end{aligned}$$

Fix an orthonormal basis  $\{|q\rangle\}_{q \in Q}$  of  $\mathcal{H}^{a_0}$ . Let  $\Gamma_{L,q}$  and  $\Gamma_{R,q}$  be linear isometries that embed  $\mathcal{M}_q$  into  $\mathcal{H}^{a_L}$  and  $\mathcal{N}_q$  into  $\mathcal{H}^{a_R}$ , respectively, and define  $P_q$  as the projection onto  $\mathcal{M}_q \otimes \mathcal{N}_q \subseteq \mathcal{H}^A$  for each  $q$ . Then  $\mathcal{H}^A$  is embedded into the Hilbert space  $\mathcal{H}^{a_0} \otimes \mathcal{H}^{a_L} \otimes \mathcal{H}^{a_R}$  by a linear isometry  $\Gamma : \mathcal{H}^A \rightarrow \mathcal{H}^{a_0} \otimes \mathcal{H}^{a_L} \otimes \mathcal{H}^{a_R}$ , defined by

$$\Gamma := \sum_{q \in Q} |q\rangle^{a_0} \otimes (\Gamma_{L,q} \otimes \Gamma_{R,q}) P_q.$$

With this embedding,  $U_g$  in (21) and a symmetric state  $\sigma$  in (22) take the forms of

$$\Gamma U_g \Gamma^\dagger = \sum_{q \in Q} |q\rangle\langle q|^{a_0} \otimes u_{g,q}^{a_L} \otimes I_q^{a_R}, \quad (23)$$

$$\Gamma \sigma \Gamma^\dagger = \sum_{q \in Q} p_q |q\rangle\langle q|^{a_0} \otimes \pi_q^{a_L} \otimes \sigma_q^{a_R}.$$

By (23) and Schur's lemma, the action of the twirling operation  $\mathcal{T}$  defined by (1) is represented as

$$\Gamma \mathcal{T}(\rho) \Gamma^\dagger = \sum_q p_q |q\rangle\langle q|^{a_0} \otimes \pi_q^{a_L} \otimes \rho_q^{a_R} \quad (24)$$

for

$$p_q = \text{Tr} [\langle q|^{a_0} \Gamma \rho \Gamma^\dagger |q\rangle^{a_0}],$$

$$\rho_q^{a_R} = p_q^{-1} \text{Tr}_{a_L} [\langle q|^{a_0} \Gamma \rho \Gamma^\dagger |q\rangle^{a_0}].$$

It is straightforward to verify that

$$S(\mathcal{T}(\rho)) = \sum_q H(\{p_q\}_q) + \sum_q p_q (S(\pi_q^{a_L}) + S(\rho_q^{a_R})). \quad (25)$$

Note also that

$$\dim \mathcal{H}^{a_0}, \dim \mathcal{H}^{a_L}, \dim \mathcal{H}^{a_R} \leq d. \quad (26)$$

### C. $n$ Identical Systems

The Hilbert space  $(\mathcal{H}^A)^{\otimes n}$  is embedded by a linear isometry  $\Gamma^{\otimes n}$  into  $(\mathcal{H}^{a_0})^{\otimes n} \otimes (\mathcal{H}^{a_L})^{\otimes n} \otimes (\mathcal{H}^{a_R})^{\otimes n}$ . For simplicity, we introduce notations

$$\mathcal{H}^{\bar{a}_0} := (\mathcal{H}^{a_0})^{\otimes n}, \quad \mathcal{H}^{\bar{a}_L} := (\mathcal{H}^{a_L})^{\otimes n}, \quad \mathcal{H}^{\bar{a}_R} := (\mathcal{H}^{a_R})^{\otimes n}. \quad (27)$$

In the same way as (23) and (24),  $U_{\vec{g}}$  and  $\mathcal{T}^{\otimes n}(\rho)$  take the forms of

$$\Gamma^{\otimes n} U_{\vec{g}} \Gamma^{\dagger \otimes n} = \sum_{\vec{q} \in Q^n} |\vec{q}\rangle\langle \vec{q}|^{\bar{a}_0} \otimes u_{\vec{g},\vec{q}}^{\bar{a}_L} \otimes I_{\vec{q}}^{\bar{a}_R}, \quad (28)$$

$$\Gamma^{\otimes n} \mathcal{T}^{\otimes n}(\rho) \Gamma^{\dagger \otimes n} = \sum_{\vec{q} \in Q^n} p_{\vec{q}} |\vec{q}\rangle\langle \vec{q}|^{\bar{a}_0} \otimes \pi_{\vec{q}}^{\bar{a}_L} \otimes \rho_{\vec{q}}^{\bar{a}_R}. \quad (29)$$

Here, we introduced notations

$$\vec{q} := q_1 \cdots q_n,$$

$$u_{\vec{g},\vec{q}} := u_{g_1,q_1} \otimes \cdots \otimes u_{g_n,q_n},$$

$$I_{\vec{q}} := I_{q_1} \otimes \cdots \otimes I_{q_n},$$

$$\pi_{\vec{q}} := \pi_{q_1} \otimes \cdots \otimes \pi_{q_n},$$

and defined

$$p_{\vec{q}} := \text{Tr} [\langle \vec{q}|^{\bar{a}_0} \Gamma^{\otimes n} \rho \Gamma^{\dagger \otimes n} |\vec{q}\rangle^{\bar{a}_0}],$$

$$\rho_{\vec{q}} := p_{\vec{q}}^{-1} \text{Tr}_{\bar{a}_L} [\langle \vec{q}|^{\bar{a}_0} \Gamma^{\otimes n} \rho \Gamma^{\dagger \otimes n} |\vec{q}\rangle^{\bar{a}_0}]$$

for  $\vec{q} \in Q^n$ .

## VI. PROOF OF ACHIEVABILITY

The direct part of Theorem 2 is formulated by the following inequality:

$$C_{\text{sym}}(\rho) \leq D_{\text{fr}}(\rho). \quad (30)$$

We prove this inequality by showing that a rate  $R$  is achievable if  $R > D_{\text{fr}}(\rho)$ . The proof proceeds along the similar line as the proof of Proposition 2 in [16], which uses the operator Chernoff bound as a key mathematical ingredient. In the following, we fix arbitrary  $\epsilon, \delta > 0$  and choose sufficiently large  $n \in \mathbb{N}$ . We denote  $\Gamma \rho \Gamma^\dagger$  by  $\tilde{\rho}$ , and follow the notations (27).

### 1. Notations

Let us first introduce notations that will be used in the proof of Inequality (30). See Appendix B for definitions and properties of typical sequences and subspaces.

- $\mathcal{H}_{n,\delta} \subset \mathcal{H}^{\bar{a}_0} \otimes \mathcal{H}^{\bar{a}_L} \otimes \mathcal{H}^{\bar{a}_R}$ : the  $\delta$ -weakly typical subspace with respect to  $\tilde{\rho}$
- $\Pi_{n,\delta}$ : the projection onto  $\mathcal{H}_{n,\delta}$
- $\{p_q\}_{q \in Q}$ : a probability distribution on  $Q$  defined by  $p_q = \text{Tr} [\langle q|^{a_0} \tilde{\rho} |q\rangle^{a_0}]$
- $\rho_q$ : a state on  $a_L a_R$  defined by  $\rho_q = p_q^{-1} \langle q|^{a_0} \tilde{\rho} |q\rangle^{a_0}$
- $\{p_{\vec{q}}\}_{\vec{q} \in Q^n}$ : a probability distribution on  $Q^n$  defined by  $p_{\vec{q}} = p_{q_1} \times \cdots \times p_{q_n}$  for  $\vec{q} = q_1 \cdots q_n$
- $\rho_{\vec{q}}$ : a state on  $\bar{a}_L \bar{a}_R$  defined by  $\rho_{\vec{q}} = \rho_{q_1} \otimes \cdots \otimes \rho_{q_n}$  for  $\vec{q} = q_1 \cdots q_n$
- $\mathcal{T}_{n,\delta}^* \in Q^n$ : the  $\delta$ -strongly typical set with respect to  $\{p_q\}_{q \in Q}$
- $\Pi_{n,\delta}^*$ : a projection operator on  $\mathcal{H}^{\bar{a}_0}$  defined by

$$\Pi_{n,\delta}^* := \sum_{\vec{q} \in \mathcal{T}_{n,\delta}^*} |\vec{q}\rangle\langle \vec{q}| \quad (31)$$

- $\mathcal{H}_{\vec{q},\delta}^{\bar{a}_R} \subset \mathcal{H}^{\bar{a}_R}$ : the  $\delta$ -conditionally typical subspace corresponding to an ensemble  $\{p_q, \rho_q^{a_R}\}_{q \in Q}$  and a sequence  $\vec{q} \in \mathcal{T}_{n,\delta}^*$
- $\Pi_{\vec{q},\delta}^{\bar{a}_R}$ : the projection onto  $\mathcal{H}_{\vec{q},\delta}^{\bar{a}_R} \subset \mathcal{H}^{\bar{a}_R}$
- $D_{\vec{q},\delta}$ : the dimension of  $\mathcal{H}_{\vec{q},\delta}^{\bar{a}_R}$ , which satisfies

$$D_{\vec{q},\delta} \leq 2^{n \sum_{q \in Q} (p_q + \delta/|Q|)(S(\rho_q^{a_R}) + \delta)} \quad (32)$$

- $\hat{\Pi}_{n,\delta}$ : a projection operator on  $\mathcal{H}^{\bar{a}_0} \otimes \mathcal{H}^{\bar{a}_L} \otimes \mathcal{H}^{\bar{a}_R}$  defined by

$$\hat{\Pi}_{n,\delta} := \sum_{\vec{q} \in \mathcal{T}_{n,\delta}^*} |\vec{q}\rangle\langle \vec{q}|^{\bar{a}_0} \otimes I_{\vec{q}}^{\bar{a}_L} \otimes \Pi_{\vec{q},\delta}^{\bar{a}_R} \quad (33)$$

- $\hat{\rho}_{n,\delta}$  : a subnormalized state on  $\bar{a}_0\bar{a}_L\bar{a}_R$  defined by

$$\hat{\rho}_{n,\delta} := \hat{\Pi}_{n,\delta} \Pi_{n,\delta} \tilde{\rho}^{\otimes n} \Pi_{n,\delta} \hat{\Pi}_{n,\delta} \quad (34)$$

- $\{\hat{p}_{\vec{q},\delta}\}_{\vec{q} \in \mathcal{T}_{n,\delta}^*}$  : a subnormalized probability distribution on  $\mathcal{T}_{n,\delta}^*$  defined by

$$\hat{p}_{\vec{q},\delta} := \text{Tr} [\langle \vec{q} |^{\bar{a}_0} \hat{\rho}_{n,\delta} | \vec{q} \rangle^{\bar{a}_0}] \quad (35)$$

- $\hat{\rho}_{\vec{q},\delta}$  : a state on  $\bar{a}_L\bar{a}_R$  defined by

$$\hat{\rho}_{\vec{q},\delta} := \hat{p}_{\vec{q},\delta}^{-1} \langle \vec{q} |^{\bar{a}_0} \hat{\rho}_{n,\delta} | \vec{q} \rangle^{\bar{a}_0} \quad (36)$$

- $\mathcal{T}'_{n,\delta} \in \mathcal{T}_{n,\delta}^*$  : a subset of  $\mathcal{T}_{n,\delta}^*$  defined by

$$\mathcal{T}'_{n,\delta} := \{\vec{q} \mid \vec{q} \in \mathcal{T}_{n,\delta}^*, \hat{p}_{\vec{q},\delta} \geq \epsilon/|\mathcal{T}_{n,\delta}^*|\} \quad (37)$$

- $\mathcal{H}'_{\vec{q},\delta} \subset \mathcal{H}_{\vec{q},\delta}^{\bar{a}_R}$  : a subspace of  $\mathcal{H}_{\vec{q},\delta}^{\bar{a}_R}$  spanned by eigenvectors of  $\hat{\rho}_{\vec{q},\delta}^{\bar{a}_R}$  with eigenvalues not smaller than  $\epsilon/D_{\vec{q},\delta}$

- $\check{\Pi}_{\vec{q},\delta}$  : the projection onto  $\mathcal{H}'_{\vec{q},\delta}$

- $\check{\Pi}_{n,\delta}$  : a projection operator on  $\mathcal{H}^{\bar{a}_0} \otimes \mathcal{H}^{\bar{a}_L} \otimes \mathcal{H}^{\bar{a}_R}$  defined by

$$\check{\Pi}_{n,\delta} := \sum_{\vec{q} \in \mathcal{T}'_{n,\delta}} |\vec{q}\rangle\langle\vec{q}|^{\bar{a}_0} \otimes I_{\vec{q}}^{\bar{a}_L} \otimes \check{\Pi}_{\vec{q},\delta}^{\bar{a}_R} \quad (38)$$

- $\check{\rho}_{\vec{q},\delta}$  : a subnormalized state on  $\bar{a}_L\bar{a}_R$  defined by

$$\check{\rho}_{\vec{q},\delta} := (I^{\bar{a}_L} \otimes \check{\Pi}_{\vec{q},\delta}^{\bar{a}_R}) \hat{\rho}_{\vec{q},\delta} (I^{\bar{a}_L} \otimes \check{\Pi}_{\vec{q},\delta}^{\bar{a}_R}) \quad (39)$$

- $\check{\rho}_{n,\delta}$  : a subnormalized state on  $\bar{a}_0\bar{a}_L\bar{a}_R$  defined by

$$\check{\rho}_{n,\delta} := \check{\Pi}_{n,\delta} \hat{\rho}_{n,\delta} \check{\Pi}_{n,\delta} \quad (40)$$

- $\zeta_{\vec{q},\vec{q}',\delta}$  : a linear operator on  $\mathcal{H}^{\bar{a}_L} \otimes \mathcal{H}^{\bar{a}_R}$  defined by

$$\zeta_{\vec{q},\vec{q}',\delta} := \langle \vec{q} | \check{\rho}_{n,\delta} | \vec{q}' \rangle$$

The following relations immediately follow from the above definitions. First, due to the definition of the typical set, we have

$$|\mathcal{T}_{n,\delta}^*| \leq 2^{n(H(\{p_q\}_q) + \delta H'(\{p_q\}_q))}, \quad (41)$$

where

$$H'(\{p_q\}_q) := -\frac{1}{|Q|} \sum_{q \in Q, p_q > 0} \log p_q < \infty. \quad (42)$$

Second, due to the definition of the typical subspace, we have

$$2^{n(S(\rho) - \delta)} \cdot \Pi_{n,\delta} \tilde{\rho}^{\otimes n} \Pi_{n,\delta} \leq \Pi_{n,\delta}.$$

Combining this with (34) and (40), we obtain

$$\begin{aligned} 2^{n(S(\rho) - \delta)} \cdot \hat{\rho}_{n,\delta} &\leq \hat{\Pi}_{n,\delta}, \\ 2^{n(S(\rho) - \delta)} \cdot \check{\rho}_{n,\delta} &\leq \check{\Pi}_{n,\delta}. \end{aligned} \quad (43)$$

Equality (39) implies

$$\check{\rho}_{\vec{q},\delta}^{\bar{a}_R} := \text{Tr}_{\bar{a}_L} [\check{\rho}_{\vec{q},\delta}] \geq \frac{\epsilon}{D_{\vec{q},\delta}} \check{\Pi}_{\vec{q},\delta}.$$

We also have

$$\hat{p}_{\vec{q},\delta} = \text{Tr} [\langle \vec{q} |^{\bar{a}_0} \check{\rho}_{n,\delta} | \vec{q} \rangle^{\bar{a}_0}], \quad \check{\rho}_{\vec{q},\delta} = \hat{p}_{\vec{q},\delta}^{-1} \langle \vec{q} |^{\bar{a}_0} \check{\rho}_{n,\delta} | \vec{q} \rangle^{\bar{a}_0}$$

and

$$\begin{aligned} \check{\rho}_{n,\delta} &= \sum_{\vec{q} \in \mathcal{T}'_{n,\delta}} \hat{p}_{\vec{q},\delta} |\vec{q}\rangle\langle\vec{q}|^{\bar{a}_0} \otimes \check{\rho}_{\vec{q},\delta}^{\bar{a}_R} \\ &\quad + \sum_{\substack{\vec{q}, \vec{q}' \in \mathcal{T}'_{n,\delta} \\ \vec{q} \neq \vec{q}'}} |\vec{q}\rangle\langle\vec{q}'|^{\bar{a}_0} \otimes \zeta_{\vec{q},\vec{q}',\delta}^{\bar{a}_L\bar{a}_R}. \end{aligned} \quad (44)$$

## 2. Evaluation of the Trace Distance

Let us evaluate the trace distance between  $\check{\rho}_{n,\delta}$  and  $\rho^{\otimes n}$ . First, due to the properties of the typical sequences and subspaces, we have

$$\text{Tr} [\Pi_{n,\delta} \tilde{\rho}^{\otimes n}] \geq 1 - \epsilon \geq 1 - 2\epsilon, \quad (45)$$

$$\text{Tr} [(\Pi_{n,\delta}^* \otimes I^{\bar{a}_L\bar{a}_R}) \tilde{\rho}^{\otimes n}] = \sum_{\vec{q} \in \mathcal{T}_{n,\delta}^*} p_{\vec{q}} \geq 1 - \epsilon, \quad (46)$$

and

$$\text{Tr} [(I_{\vec{q}}^{\bar{a}_L} \otimes \Pi_{\vec{q},\delta}^{\bar{a}_R}) \check{\rho}_{\vec{q},\delta}^{\bar{a}_L\bar{a}_R}] \geq 1 - \epsilon \quad (47)$$

for each  $\vec{q} \in \mathcal{T}_{n,\delta}^*$ . From (33), (46) and (47), we obtain

$$\begin{aligned} \text{Tr} [\hat{\Pi}_{n,\delta} \tilde{\rho}^{\otimes n}] &= \sum_{\vec{q} \in \mathcal{T}_{n,\delta}^*} p_{\vec{q}} \text{Tr} [(I_{\vec{q}}^{\bar{a}_L} \otimes \Pi_{\vec{q},\delta}^{\bar{a}_R}) \check{\rho}_{\vec{q},\delta}^{\bar{a}_L\bar{a}_R}] \\ &\geq \sum_{\vec{q} \in \mathcal{T}_{n,\delta}^*} p_{\vec{q}} (1 - \epsilon) \geq 1 - 2\epsilon. \end{aligned} \quad (48)$$

Applying Lemma 4 in Appendix A 2 to (34), (45) and (48) yields

$$\text{Tr} [\hat{\rho}_{n,\delta}] = \text{Tr} [\hat{\Pi}_{n,\delta} \Pi_{n,\delta} \tilde{\rho}^{\otimes n} \Pi_{n,\delta} \hat{\Pi}_{n,\delta}] \geq 1 - 2\sqrt{2\epsilon} \quad (49)$$

and

$$\left\| \frac{\hat{\rho}_{n,\delta}}{\text{Tr} [\hat{\rho}_{n,\delta}]} - \tilde{\rho}^{\otimes n} \right\|_1 \leq 5\sqrt[4]{2\epsilon}. \quad (50)$$

From (31), (35), Inequality (A1) in Appendix A 1, (49), (46) and (50), we have

$$\begin{aligned}
\sum_{\vec{q} \in \mathcal{T}_{n,\delta}^*} \hat{p}_{\vec{q},\delta} &= \text{Tr} \left[ (\Pi_{n,\delta}^{*\bar{a}_0} \otimes I^{\bar{a}_L \bar{a}_R}) \hat{\rho}_{n,\delta} \right] \\
&= \text{Tr} [\hat{\rho}_{n,\delta}] \cdot \text{Tr} \left[ (\Pi_{n,\delta}^{*\bar{a}_0} \otimes I^{\bar{a}_L \bar{a}_R}) \frac{\hat{\rho}_{n,\delta}}{\text{Tr} [\hat{\rho}_{n,\delta}]} \right] \\
&\geq \text{Tr} [\hat{\rho}_{n,\delta}] \times \\
&\quad \left( \text{Tr} \left[ (\Pi_{n,\delta}^{*\bar{a}_0} \otimes I^{\bar{a}_L \bar{a}_R}) \tilde{\rho}^{\otimes n} \right] - \frac{1}{2} \left\| \frac{\hat{\rho}_{n,\delta}}{\text{Tr} [\hat{\rho}_{n,\delta}]} - \tilde{\rho}^{\otimes n} \right\|_1 \right) \\
&\geq (1 - 2\sqrt{2}\epsilon)(1 - \epsilon - 5\sqrt[4]{2}\epsilon) \geq 1 - 8\sqrt[4]{2}\epsilon. \quad (51)
\end{aligned}$$

It is straightforward to verify from (39) and (36) that

$$\begin{aligned}
\text{Tr} [\check{\rho}_{\vec{q},\delta}] &= \text{Tr} \left[ (I^{\bar{a}_L} \otimes \check{\Pi}_{\vec{q},\delta}^{\bar{a}_R}) \hat{\rho}_{\vec{q},\delta} \right] = \text{Tr} [\check{\Pi}_{\vec{q},\delta} \hat{\rho}_{\vec{q},\delta}^{\bar{a}_R}] \\
&= 1 - \text{Tr} \left[ (I - \check{\Pi}_{\vec{q},\delta}) \hat{\rho}_{\vec{q},\delta}^{\bar{a}_R} \right] \\
&\geq 1 - D_{\vec{q},\delta} \cdot \frac{\epsilon}{D_{\vec{q},\delta}} = 1 - \epsilon. \quad (52)
\end{aligned}$$

From (40), (44), (52), (51) and (37), we have

$$\begin{aligned}
\text{Tr} [\check{\Pi}_{n,\delta} \hat{\rho}_{n,\delta}] &= \text{Tr} [\check{\rho}_{n,\delta}] = \sum_{\vec{q} \in \mathcal{T}_{n,\delta}'} \hat{p}_{\vec{q},\delta} \text{Tr} [\check{\rho}_{\vec{q},\delta}] \\
&\geq (1 - \epsilon) \sum_{\vec{q} \in \mathcal{T}_{n,\delta}'} \hat{p}_{\vec{q},\delta} \\
&= (1 - \epsilon) \left( \sum_{\vec{q} \in \mathcal{T}_{n,\delta}^*} \hat{p}_{\vec{q},\delta} - \sum_{\vec{q} \in \mathcal{T}_{n,\delta}' \setminus \mathcal{T}_{n,\delta}^*} \hat{p}_{\vec{q},\delta} \right) \\
&\geq (1 - \epsilon)(1 - 8\sqrt[4]{2}\epsilon - \epsilon) \geq 1 - 10\sqrt[4]{2}\epsilon,
\end{aligned}$$

which implies

$$\text{Tr} \left[ \check{\Pi}_{n,\delta} \frac{\hat{\rho}_{n,\delta}}{\text{Tr} [\hat{\rho}_{n,\delta}]} \right] \geq \text{Tr} [\check{\Pi}_{n,\delta} \hat{\rho}_{n,\delta}] \geq 1 - 10\sqrt[4]{2}\epsilon.$$

Due to (40) and the gentle measurement lemma (see Appendix A 2), the above inequality leads to

$$\left\| \frac{\check{\rho}_{n,\delta}}{\text{Tr} [\check{\rho}_{n,\delta}]} - \frac{\hat{\rho}_{n,\delta}}{\text{Tr} [\hat{\rho}_{n,\delta}]} \right\|_1 \leq 2\sqrt{10}\sqrt[8]{2}\epsilon \leq 8\sqrt[8]{2}\epsilon.$$

Combining this with Inequality (50), we obtain

$$\left\| \frac{\check{\rho}_{n,\delta}}{\text{Tr} [\check{\rho}_{n,\delta}]} - \tilde{\rho}^{\otimes n} \right\|_1 \leq 5\sqrt[4]{2}\epsilon + 8\sqrt[8]{2}\epsilon \leq 13\sqrt[8]{2}\epsilon \quad (53)$$

by the triangle inequality.

### 3. Construction of Random Unitary Operations

Consider a unitary (5) for  $\vec{g} := (g_1, \dots, g_n) \in G^n$ , which is decomposed by  $\Gamma^{\otimes n}$  as (28). Denote  $\Gamma^{\otimes n} U_{\vec{g}} \Gamma^{\dagger \otimes n}$  by  $\tilde{U}_{\vec{g}}$ , and define an operator

$$X_{n,\delta}(\vec{g}) := 2^{n(S(\rho)-\delta)} \tilde{U}_{\vec{g}} \check{\rho}_{n,\delta} \tilde{U}_{\vec{g}}^\dagger. \quad (54)$$

From (28), (38) and (43) we have

$$X_{n,\delta}(\vec{g}) \leq \check{\Pi}_{n,\delta}.$$

Suppose that each  $g_i$  in  $\vec{g}$  is chosen independently according to the group invariant probability measure on  $G$ . Due to (7), (29) and (44), as an ensemble average we have

$$\begin{aligned}
\bar{X}_{n,\delta} &:= \mathbb{E} [X_{n,\delta}(\vec{g})] \\
&= 2^{n(S(\rho)-\delta)} \tilde{\mathcal{T}}^{\otimes n}(\check{\rho}_{n,\delta}) \\
&= 2^{n(S(\rho)-\delta)} \sum_{\vec{q} \in \mathcal{T}_{n,\delta}'} \hat{p}_{\vec{q},\delta} |\vec{q}\rangle \langle \vec{q}|^{\bar{a}_0} \otimes \pi_{\vec{q}}^{\bar{a}_L} \otimes \check{\rho}_{\vec{q},\delta}^{\bar{a}_R}, \quad (55)
\end{aligned}$$

where  $\tilde{\mathcal{T}}(\cdot) := \Gamma \mathcal{T}(\Gamma^\dagger(\cdot) \Gamma) \Gamma^\dagger$ . We note that, from (8),

$$\bar{\rho}_{n,\delta} := \Gamma^{\dagger \otimes n} \left( \frac{2^{-n(S(\rho)-\delta)} \bar{X}_{n,\delta}}{\text{Tr} [\check{\rho}_{n,\delta}]} \right) \Gamma^{\otimes n} \quad (56)$$

is a normalized symmetric state.

### 4. Evaluation of Eigenvalues

The minimum nonzero eigenvalue of  $\bar{X}_{n,\delta}$  in (55) is calculated as follows. First, due to (37) and (41), we have

$$\hat{p}_{\vec{q},\delta} \geq \frac{\epsilon}{|\mathcal{T}_{n,\delta}^*|} \geq \epsilon \cdot 2^{-n(H(\{p_q\}_q) + \delta H'(\{p_q\}_q))}.$$

Second, owing to  $\mathcal{T}_{n,\delta}' \subset \mathcal{T}_{n,\delta}^*$ , we have

$$\text{rank} \pi_{\vec{q}}^{\bar{a}_L} = \prod_{i=1}^n \text{rank} \pi_{q_i}^{\bar{a}_L} \leq \prod_{q \in Q} 2^{n(p_q + \delta/|Q|)S(\pi_q^{\bar{a}_L})}.$$

Thus, using (26), the nonzero eigenvalue  $\mu_{\vec{q}}$  of  $\pi_{\vec{q}}^{\bar{a}_L}$  is bounded below as

$$\begin{aligned}
\mu_{\vec{q},\delta} &\geq \prod_{q \in Q} 2^{-n(p_q + \delta/|Q|)S(\pi_q^{\bar{a}_L})} \\
&\geq 2^{-n(\sum_q p_q S(\pi_q^{\bar{a}_L}) + \delta \log d)}.
\end{aligned}$$

Third, the minimum nonzero eigenvalue  $\nu_{\vec{q}}$  of  $\check{\rho}_{\vec{q},\delta}^{\bar{a}_R}$  is, due to (39), (32) and (26), bounded below as

$$\begin{aligned}
\nu_{\vec{q},\delta} &\geq \epsilon / D_{\vec{q},\delta} \\
&\geq \epsilon \cdot 2^{-n \sum_q (p_q + \delta/|Q|)(S(\rho_q^{\bar{a}_R}) + \delta)} \\
&\geq \epsilon \cdot 2^{-n(\sum_q p_q S(\rho_q^{\bar{a}_R}) + 2\delta + \delta \log d)}.
\end{aligned}$$

The minimum nonzero eigenvalue  $\lambda$  of  $\bar{X}_{n,\delta}$  is hence bounded below as

$$\begin{aligned}
\lambda &\geq 2^{n(S(\rho)-\delta)} \cdot \min_{\vec{q} \in \mathcal{T}_{n,\delta}'} (\hat{p}_{\vec{q},\delta} \mu_{\vec{q},\delta} \nu_{\vec{q},\delta}) \\
&\geq \epsilon^2 \cdot 2^{n(S(\rho)-H(\{p_q\}_q) - \sum_q p_q (S(\pi_q^{\bar{a}_L}) + S(\rho_q^{\bar{a}_R})))} \\
&\quad \times 2^{-n(3\delta + 2\delta \log d + \delta H'(\{p_q\}_q))} \\
&= \epsilon^2 \cdot 2^{n(S(\rho) - S(\mathcal{T}(\rho)) - 3\delta - 2\delta \log d - \delta H'(\{p_q\}_q))} \\
&= \epsilon^2 \cdot 2^{-n(D_{\text{tr}}(\rho) + 3\delta + 2\delta \log d + \delta H'(\{p_q\}_q))}, \quad (57)
\end{aligned}$$

where the fourth line follows from Equality (25) and the fifth line from (10). Due to (26), We also have

$$\text{rank } \bar{X}_{n,\delta} \leq (\dim \mathcal{H}^{a_0} \times \dim \mathcal{H}^{a_L} \times \dim \mathcal{H}^{a_R})^n \leq d^{3n}.$$

### 5. Application of the Operator Chernoff Bound

Let  $N$  be a natural number, and suppose  $g_{ki}$  ( $1 \leq k \leq N, 1 \leq i \leq n$ ) are group elements in  $G$  that are randomly and independently chosen according to the group invariant probability measure. Denote  $(g_{k1}, \dots, g_{kn})$  by  $\vec{g}_k$ . Due to the operator Chernoff bound (Lemma 3 in [16]), we have

$$\Pr \left\{ \frac{1}{N} \sum_{k=1}^N X_{n,\delta}(\vec{g}_k) \notin [(1-\epsilon)\bar{X}_{n,\delta}, (1+\epsilon)\bar{X}_{n,\delta}] \right\} \leq 2d^{3n} \exp \left( -\frac{N\lambda\epsilon^2}{2} \right)$$

for any  $\epsilon \in (0, 1]$ , which implies that

$$\Pr \left\{ \left\| \frac{1}{2^{nR}} \sum_{k=1}^{2^{nR}} X_{n,\delta}(\vec{g}_k) - \bar{X}_{n,\delta} \right\|_1 \leq \epsilon \|\bar{X}_{n,\delta}\|_1 \right\} \geq 1 - 2d^{3n} \exp \left( -\frac{2^{nR}\lambda\epsilon^2}{2} \right) \quad (58)$$

for an arbitrary  $R > 0$ .

Due to (57), if  $R$  satisfies

$$R > D_{\text{fr}}(\rho) + \delta(3 + 2 \log d + H'(\{p_q\}_q)), \quad (59)$$

the R.H.S. in (58) is greater than 0 for sufficiently large  $n$ . Then there exists a set of group elements  $\{\vec{g}_k\}_{k=1}^{2^{nR}}$  such that

$$\left\| \frac{1}{2^{nR}} \sum_{k=1}^{2^{nR}} X_{n,\delta}(\vec{g}_k) - \bar{X}_{n,\delta} \right\|_1 \leq \epsilon \|\bar{X}_{n,\delta}\|_1. \quad (60)$$

For each element in the set, define  $V_k := U_{\vec{g}_k}$ . Construct a random unitary operation  $\mathcal{V}_n$  on  $A^n$  as

$$\mathcal{V}_n : \tau \rightarrow \frac{1}{2^{nR}} \sum_{k=1}^{2^{nR}} V_k \tau V_k^\dagger,$$

and define  $\tilde{\mathcal{V}}_n(\cdot) := \Gamma^{\otimes n} \mathcal{V}_n(\Gamma^{\dagger \otimes n}(\cdot) \Gamma^{\otimes n}) \Gamma^{\dagger \otimes n}$ .

### 6. Evaluation of the Total Error

Let us evaluate the total error. First, from (54), (55), (56) and (60), we have

$$\left\| \tilde{\mathcal{V}}_n \left( \frac{\tilde{\rho}_{n,\delta}}{\text{Tr}[\tilde{\rho}_{n,\delta}]} \right) - \Gamma^{\otimes n} \bar{\rho}_{n,\delta} \Gamma^{\dagger \otimes n} \right\|_1 \leq \epsilon \|\bar{\rho}_{n,\delta}\|_1 \leq \epsilon.$$

Second, from Inequality (53) and the monotonicity of the trace distance, we have

$$\left\| \tilde{\mathcal{V}}_n \left( \frac{\tilde{\rho}_{n,\delta}}{\text{Tr}[\tilde{\rho}_{n,\delta}]} \right) - \tilde{\mathcal{V}}_n(\bar{\rho}^{\otimes n}) \right\|_1 \leq 13\sqrt[8]{2}\epsilon.$$

Due to the isometry invariance of the trace distance and the triangle inequality, we obtain

$$\begin{aligned} \|\mathcal{V}_n(\rho^{\otimes n}) - \bar{\rho}_{n,\delta}\|_1 &= \|\tilde{\mathcal{V}}_n(\bar{\rho}^{\otimes n}) - \Gamma^{\otimes n} \bar{\rho}_{n,\delta} \Gamma^{\dagger \otimes n}\|_1 \\ &\leq \epsilon + 13\sqrt[8]{2}\epsilon. \end{aligned} \quad (61)$$

Since the relation (61) holds for any  $\epsilon, \delta > 0$ ,  $R$  satisfying (59) and sufficiently large  $n$ , we obtain (30). ■

## VII. CONCLUSION

In this paper, we have addressed the problem of quantifying asymmetry of quantum states from an operational point of view. We have introduced the task of symmetrization, and analyzed the minimum cost of randomness required for symmetrizing a quantum state, by considering an asymptotic limit of infinitely many copies and vanishingly small error. We prove that the minimum cost of randomness is asymptotically equal to the relative entropy of frameness.

### Acknowledgments

The authors thank Andreas Winter for helpful discussions, and Hiroyasu Tajima for useful comments on an earlier draft of this paper.

### Appendix A: Trace Distance and The Gentle Measurement Lemma

#### 1. Trace Distance

The trace distance between two quantum states  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  is defined by

$$\|\rho - \sigma\|_1 = \text{Tr} \left[ \sqrt{(\rho - \sigma)^2} \right].$$

It satisfies

$$0 \leq \|\rho - \sigma\|_1 \leq 2$$

and

$$\|\rho - \sigma\|_1 = 2 \max_{\Lambda} \text{Tr}[\Lambda(\sigma - \rho)],$$



where the maximization is taken over all linear operators  $\Lambda$  on  $\mathcal{H}$  that satisfy  $0 \leq \Lambda \leq I$ . Thus we have

$$\text{Tr}[\Pi\rho] \geq \text{Tr}[\Pi\sigma] - \frac{1}{2}\|\rho - \sigma\|_1 \quad (\text{A1})$$

for any projection operator  $\Pi$  on  $\mathcal{H}$ .

For  $\rho, \sigma, \tau \in \mathcal{S}(\mathcal{H})$ , we have

$$\|\rho - \tau\|_1 \leq \|\rho - \sigma\|_1 + \|\sigma - \tau\|_1,$$

which is called the *triangle inequality*. The trace distance is monotonically nonincreasing under quantum operations, i.e., it satisfies

$$\|\rho - \sigma\|_1 \geq \|\mathcal{E}(\rho) - \mathcal{E}(\sigma)\|_1$$

for any  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  and any linear CPTP map  $\mathcal{E} : \mathcal{S}(\mathcal{H}) \rightarrow \mathcal{S}(\mathcal{H}')$ .

## 2. Gentle Measurement Lemma

The gentle measurement lemma (Lemma 9.4.1 in [17]) states that for any  $\rho \in \mathcal{S}(\mathcal{H})$ ,  $X \in \mathcal{L}(\mathcal{H})$  and  $\epsilon \geq 0$  such that  $0 \leq X \leq I$  and  $\text{Tr}[\rho X] \geq 1 - \epsilon$ , we have

$$\left\| \rho - \frac{\sqrt{X}\rho\sqrt{X}}{\text{Tr}[\rho X]} \right\|_1 \leq 2\sqrt{\epsilon}.$$

The following lemma was obtained in [18] as a corollary.

*Lemma 4* (Lemma 32 in [18]) For any  $\rho \in \mathcal{S}(\mathcal{H})$ ,  $X, Y \in \mathcal{L}(\mathcal{H})$  and  $\delta \in [0, 1]$  such that

$$0 \leq X \leq I, \quad 0 \leq Y \leq I$$

and

$$\text{Tr}[\rho X] \geq 1 - \delta, \quad \text{Tr}[\rho Y] \geq 1 - \delta,$$

define

$$\begin{aligned} D_{XY} &:= \text{Tr}[\sqrt{Y}\sqrt{X}\rho\sqrt{X}\sqrt{Y}], \\ \rho_{XY} &:= \frac{\sqrt{Y}\sqrt{X}\rho\sqrt{X}\sqrt{Y}}{D_{XY}}. \end{aligned}$$

Then we have

$$D_{XY} \geq 1 - 2\sqrt{\delta}, \quad \|\rho - \rho_{XY}\|_1 \leq 5\sqrt[4]{\delta}.$$

## Appendix B: Typical Sequences and Subspaces

We review definitions and properties of typical sequences and subspaces. See e.g. [17, 19] for further details.

## 1. Typical Sequences

Let  $X$  be a discrete random variable with finite alphabet  $\mathcal{X}$  and probability distribution  $p_x = \Pr\{X = x\}$  where  $x \in \mathcal{X}$ . A sequence  $\vec{x} = (x_1, \dots, x_n) \in \mathcal{X}^n$  is said to be  *$\delta$ -weakly typical with respect to  $\{p_x\}_{x \in \mathcal{X}}$*  if it satisfies

$$2^{-n(H(X)+\delta)} \leq \prod_{i=1}^N p_{x_i} \leq 2^{-n(H(X)-\delta)}. \quad (\text{B1})$$

The set of all  $\delta$ -weakly typical sequences is called the  *$\delta$ -weakly typical set*, and is denoted by  $\mathcal{T}_{n,\delta}$ . Denoting  $\prod_{i=1}^N p_{x_i}$  by  $p_{\vec{x}}$ , we have

$$1 = \sum_{\vec{x} \in \mathcal{X}^n} p_{\vec{x}} \geq \sum_{\vec{x} \in \mathcal{T}_{n,\delta}} p_{\vec{x}} \geq |\mathcal{T}_{n,\delta}| \cdot 2^{-n(H(X)+\delta)},$$

which implies

$$|\mathcal{T}_{n,\delta}| \leq 2^{n(H(X)+\delta)}. \quad (\text{B2})$$

A sequence  $\vec{x} = (x_1, \dots, x_n) \in \mathcal{X}^n$  is called  *$\delta$ -strongly typical with respect to  $\{p_x\}_{x \in \mathcal{X}}$*  if it satisfies

$$\left| \frac{1}{n} N_{x|\vec{x}} - p_x \right| < \frac{\delta}{|\mathcal{X}|}$$

for all  $x \in \mathcal{X}$  and  $N_{x|\vec{x}} = 0$  if  $p_x = 0$ . Here,  $N_{x|\vec{x}}$  is the number of occurrences of the symbol  $x$  in the sequence  $\vec{x}$ . The set of all  $\delta$ -strongly typical sequences is called the  *$\delta$ -strongly typical set*, and denoted by  $\mathcal{T}_{n,\delta}^*$ . It is straightforward to verify that any  $\vec{x} \in \mathcal{T}_{n,\delta}^*$  satisfies

$$2^{-n(H(X)+\delta H'(X))} \leq \prod_{i=1}^N p_{x_i} \leq 2^{-n(H(X)-\delta H'(X))},$$

where we defined

$$H'(X) := -\frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}, p_x > 0} \log p_x.$$

Thus, in the same way as (B2), we have

$$|\mathcal{T}_{n,\delta}^*| \leq 2^{n(H(X)+\delta H'(X))}.$$

The weak law of large numbers implies that

$$\begin{aligned} \Pr\{(X_1, \dots, X_n) \in \mathcal{T}_{n,\delta}\} &\geq 1 - \epsilon, \\ \Pr\{(X_1, \dots, X_n) \in \mathcal{T}_{n,\delta}^*\} &\geq 1 - \epsilon \end{aligned} \quad (\text{B3})$$

for any  $\epsilon, \delta > 0$  and sufficiently large  $n$ .

Let  $X$  and  $Y$  be discrete random variables with finite alphabets  $\mathcal{X}$  and  $\mathcal{Y}$ , respectively, with probability distribution  $p_{x,y} = \Pr\{X = x, Y = y\}$  where  $(x, y) \in \mathcal{X} \times \mathcal{Y}$ . For any  $\vec{x} \in \mathcal{T}_{n,\delta}^*$ , a sequence  $\vec{y} = (y_1, \dots, y_n) \in$

$\mathcal{Y}^n$  is said to be  $\delta$ -conditionally typical with respect to  $\{p_{x,y}\}_{(x,y) \in \mathcal{X} \times \mathcal{Y}}$  and  $\vec{x}$  if it satisfies

$$\prod_{x \in \mathcal{X}} 2^{-n(p_x + \delta/|\mathcal{X}|)(H(Y|X=x) + \delta)} \leq \prod_{i=1}^N p_{y_i|x_i} \leq \prod_{x \in \mathcal{X}} 2^{-n(p_x - \delta/|\mathcal{X}|)(H(Y|X=x) - \delta)}.$$

Here,  $p_{y|x}$  is the conditional probability defined by  $p_{y|x} := p_{x,y}/p_x$ , and  $H(Y|X)$  is the conditional entropy defined by

$$H(Y|X) := - \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} p_x p_{y|x} \log p_{y|x}.$$

The set of all  $\delta$ -conditionally typical sequences is called the  $\delta$ -conditionally typical set, and is denoted by  $\mathcal{T}_{\vec{x},\delta}$  for each  $\vec{x} \in \mathcal{T}_{n,\delta}^*$ . Denoting  $\prod_{i=1}^N p_{y_i|x_i}$  by  $p_{\vec{y}|\vec{x}}$ , we have

$$1 = \sum_{\vec{y} \in \mathcal{Y}^n} p_{\vec{y}|\vec{x}} \geq \sum_{\vec{y} \in \mathcal{T}_{\vec{x},\delta}} p_{\vec{y}|\vec{x}} \geq |\mathcal{T}_{\vec{x},\delta}| \cdot \prod_{x \in \mathcal{X}} 2^{-n(p_x + \delta/|\mathcal{X}|)(H(Y|X=x) + \delta)},$$

which implies that

$$|\mathcal{T}_{\vec{x},\delta}| \leq \prod_{x \in \mathcal{X}} 2^{n(p_x + \delta/|\mathcal{X}|)(H(Y|X=x) + \delta)}. \quad (\text{B4})$$

Due to the weak law of large numbers, we have

$$\Pr\{(Y_1, \dots, Y_n) \in \mathcal{T}_{\vec{x},\delta}^* | (X_1, \dots, X_n) = \vec{x}\} \geq 1 - \epsilon \quad (\text{B5})$$

for any  $\epsilon, \delta > 0$ , sufficiently large  $n$  and  $\vec{x} \in \mathcal{T}_{n,\delta}^*$ .

## 2. Typical Subspaces

Suppose the spectral decomposition of  $\rho \in \mathcal{S}(\mathcal{H})$  is given by  $\rho = \sum_{x \in \mathcal{X}} p_x |x\rangle\langle x|$ . The  $\delta$ -weakly typical sub-

space  $\mathcal{H}_{n,\delta} \subset \mathcal{H}^{\otimes n}$  with respect to  $\rho$  is defined as

$$\mathcal{H}_{n,\delta} := \text{span}\{|x_1\rangle \cdots |x_n\rangle \in \mathcal{H}^{\otimes n} | (x_1, \dots, x_n) \in \mathcal{T}_{n,\delta}\},$$

where  $\mathcal{T}_{n,\delta}$  is the  $\delta$ -weakly typical set with respect to  $\{p_x\}_x$ . Let  $\Pi_{n,\delta}$  be the projection onto  $\mathcal{H}_{n,\delta}$ . From (B2), we have

$$\dim \mathcal{H}_{n,\delta} \leq 2^{n(S(\rho) + \delta)}.$$

For any  $\epsilon, \delta > 0$  and sufficiently large  $n$ , we have

$$\text{Tr}[\Pi_{n,\delta} \rho^{\otimes n}] = \sum_{\vec{x} \in \mathcal{T}_{n,\delta}} p_{\vec{x}} \geq 1 - \epsilon$$

from (B3).

Consider an ensemble of quantum states  $\{p_x, \rho_x\}_{x \in \mathcal{X}}$  on system  $A$ , and suppose the spectral decomposition of  $\rho_x$  is given by  $\rho_x = \sum_{y \in \mathcal{Y}} p_{y|x} |y; x\rangle\langle y; x|$  for each  $x \in \mathcal{X}$ . The  $\delta$ -conditionally typical subspace  $\mathcal{H}_{\vec{x},\delta} \subset \mathcal{H}^{\otimes n}$  with respect to  $\{p_x, \rho_x\}_{x \in \mathcal{X}}$  and a sequence  $\vec{x} = (x_1, \dots, x_n) \in \mathcal{T}_{n,\delta}^*$  is defined as

$$\mathcal{H}_{\vec{x},\delta} := \text{span}\{|y_1; x_1\rangle \cdots |y_n; x_n\rangle \in \mathcal{H}^{\otimes n} | (y_1, \dots, y_n) \in \mathcal{T}_{\vec{x},\delta}\},$$

where  $\mathcal{T}_{\vec{x},\delta}$  is the  $\delta$ -conditionally typical set with respect to  $\{p_x p_{y|x}\}_{(x,y) \in \mathcal{X} \times \mathcal{Y}}$  and  $\vec{x} \in \mathcal{T}_{n,\delta}^*$ . Let  $\Pi_{\vec{x},\delta}$  be the projection onto  $\mathcal{H}_{\vec{x},\delta}$ . From (B4), we have

$$\dim \mathcal{H}_{\vec{x},\delta} \leq 2^{n \sum_x (p_x + \delta/|\mathcal{X}|)(S(\rho_x) + \delta)}.$$

Let us denote  $\rho_{x_1} \otimes \cdots \otimes \rho_{x_n}$  by  $\rho_{\vec{x}}$  for  $\vec{x} = x_1 \cdots x_n$ . For any  $\epsilon, \delta > 0$ , sufficiently large  $n$  and  $\vec{x} \in \mathcal{T}_{n,\delta}^*$  we have

$$\text{Tr}[\Pi_{\vec{x},\delta} \rho_{\vec{x}}] = \sum_{\vec{y} \in \mathcal{T}_{\vec{x},\delta}} p_{\vec{y}|\vec{x}} \geq 1 - \epsilon$$

from (B5).

- 
- [1] V. Giovannetti, S. Lloyd, and L. Maccone, Nat. Photon. **5**, 222 (2011).
  - [2] M. J. W. Hall and H. M. Wiseman, Phys. Rev. X **2**, 041006 (2012).
  - [3] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. A **70**, 032307 (2004).
  - [4] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. **79**, 555 (2007).
  - [5] I. Marvian and R. B. Mann, Phys. Rev. A **78**, 022304 (2008).
  - [6] J.-C. Boileau, L. Sheridan, M. Laforest, and S. D. Bartlett, J. Math. Phys. **49**, 032105 (2008).
  - [7] S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner, New J. of Phys. **11**, 063013 (2009).
  - [8] J. A. Vaccaro, F. Anselmi, H. M. Wiseman, and K. Jacobs, Phys. Rev. A **77**, 032114 (2008).
  - [9] G. Gour and R. W. Spekkens, New J. of Phys. **10**, 033023 (2007).
  - [10] G. Gour, I. Marvian, and R. W. Spekkens, Phys. Rev. A **80**, 012307 (2008).
  - [11] M. Skotiniotis and G. Gour, New J. of Phys. **14**, 073022 (2012).
  - [12] M. Piani, M. Cianciaruso, T. R. Bromley, C. Napoli, N. Johnston, and G. Adesso, Phys. Rev. A **93**, 042107 (2016).
  - [13] I. Marvian and R. W. Spekkens, Nat. Comm. **5**, 3821 (2014).

- (2014).
- [14] G. Gour and R. W. Spekkens, *Erasing quantum coherence: An operational approach*, e-print arXiv:1506.08186.
  - [15] M. Fannes, Comm. Math. Phys. **31**, 291 (1973).
  - [16] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A **72**, 032317 (2005).
  - [17] M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).
  - [18] E. Wakakuwa, A. Soeda, and M. Murao, *A coding theorem for bipartite unitaries in distributed quantum computation*, e-print arXiv:1505.4352v2.
  - [19] T. M. Cover and J. A. Thomas, *Elements of Information Theory (2nd ed.)* (Wiley-Interscience, 2005).